Adam E. Polk (SBN 273000)
Simon S. Grille (SBN 294914)
Kimberly Macey (SBN 342019)
Reid Gaa (SBN 330141)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com
rgaa@girardsharp.com

Attorneys for Plaintiffs

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@milberg.com

Gary M. Klinger (*pro hac vice* forthcoming)
Alexandra M. Honeycutt (*pro hac vice* forthcoming)
Nick Suciu (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
ahoneycutt@milberg.com
nsuciu@milberg.com

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

In re Meta Browser Tracking Litigation

Case No. 4:22-cv-05267-JST

JURY DEMAND

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Gabriele Willis, Shelby Cooper, Rama Kolesnikow, Lisa Bush, David Alzate, Mark Letoski, Louis Green, Ed Rennie, Teia Pittman, Raven Johnson, Chanel Robinson, Kevin Zenstein, Mary Thew, and Lisa Evans, on behalf of the Class and Subclasses defined below, bring this action against Meta Platforms, Inc. ("Meta") and allege as follows:

NATURE OF THE ACTION

1. Plaintiffs are Facebook users whose online activity Meta surreptitiously tracked without their knowledge or consent. Plaintiffs bring this action on behalf of themselves and other Facebook users to recover damages for—and put a stop to—the conduct in question.

2. Meta owns and operates Facebook, one of the world's largest social media platforms, which Plaintiffs and Class Members use. Meta tracked their web-browsing activity on their iPhones and iPads ("Apple Devices"), even on websites displaying or requiring the disclosure of financial and health information, in granular detail, down to the keystroke. No Plaintiff consented to Meta monitoring and profiting from their private browsing activity, messages, and other information they communicated online. Even though each Plaintiff chose *not* to be tracked—and Meta knew of this preference—it nonetheless tracked their activity on and across third-party websites.

3. Meta's lucrative mobile advertising business relies on tracking people through their personal devices and building comprehensive profiles that advertisers use to precisely target desired individuals or demographics with algorithmically placed ads. Meta's enormous user base and possession of data regarding their online activity has enabled it to reap billions in digital advertising revenue for years.

4. Beginning in April 2021, in a change that Apple Inc. touted as protecting user privacy, Apple updated its operating systems for iPhones ("iOS") and iPads ("iPadOS").[1] The update required app developers, like Meta, to obtain users' express consent before tracking their activity on third-party websites for the purposes of advertising or sharing the information with data brokers. Apple presented the choice through a pop-up window asking users if they wanted to opt in to being tracked across other companies' websites. Unsurprisingly, the overwhelming majority of users chose not to be tracked.

[1] As used in this Complaint, iOS means both iOS and iPadOS; the latter is the operating system for Apple iPad devices, and is identical to iOS in all respects material to this Complaint.

Almost overnight, Meta lost access to a key source of data derived from observing Apple Device users while they accessed third-party websites and communicated information, including sensitive financial, health, and other private information, by typing into search boxes, forms, and other fields. With its user tracking ability neutralized, Meta lost billions of dollars in potential advertising revenue.

5. Confronted with the imperative to regain this data and lost revenue, Meta devised a technical workaround allowing it to track its users' activity and communications on third-party websites opened via the Facebook app, even where users expressed their preference not to be tracked on their Apple Device. When a person using the Facebook app clicks on a link to an ostensibly external third-party website, Meta causes the link to be opened in an in-app browser—i.e., on Facebook's own platform—instead of the smartphone's default browser. Meta never tells users they are being tracked through an in-app browser.

6. Meta's surveilling of citizens' private communications and other confidential browsing activity, contrary to their stated preference, violates federal and state privacy and other laws. Plaintiffs and Class Members seek appropriate damages or restitution as well as injunctive relief to halt Meta's undisclosed tracking of Apple users who did not wish to be tracked.

JURISDICTION, VENUE AND CHOICE OF LAW

7. The Court has personal jurisdiction over Meta because it is headquartered in this District.

8. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiffs' claims arise in part under federal law: the Wiretap Act, 18 U.S.C. § 2510 *et seq*., and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq*. The Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d) because there are more than 100 Class Members, the amount in controversy exceeds $5 million (excluding interest and costs), and at least one Class Member is a citizen of a state different from Meta's state of domicile. The Court has supplemental jurisdiction over Plaintiffs' state-law claims under 28 U.S.C. § 1367.

9. Venue is proper under 28 U.S.C. § 1391 because Meta is headquartered in his District.

10. There is a significant aggregation of contacts between Meta's conduct and California. Meta is headquartered and does substantial business in California. Further, a significant percentage of Class Members are located in, and Meta aimed a significant portion of its illicit conduct at, California.

The conduct that forms the basis for each Class Member's claims against Meta emanated from its headquarters in Menlo Park, California. Numerous communications that Meta illegally intercepted were between Class Members and third-party websites controlled and maintained and with servers based in California. Moreover, Meta devised and executed its wrongful conduct, wrote the software code at issue, planned its communications with Class Members, and set its relevant policies and practices at its Menlo Park headquarters. California thus has a greater interest than any other state in applying its law to the claims in this case.

11. California has a very strong interest in preventing its resident corporations, such as Meta, from deceiving and invading the privacy of consumers and in ensuring that the harm inflicted on such consumers is adequately redressed. California's interest in preventing unlawful corporate behavior occurring in California substantially outweighs any interest of any other state in denying recovery to its residents injured by an out-of-state defendant or in applying its laws to business decisions and practices occurring outside its borders. If other states' laws were applied to Class Members' claims, California's strong interest in deterring resident corporations from committing unfair or deceptive trade practices would be significantly impaired.

DIVISIONAL ASSIGNMENT

12. Pursuant to Civil Local Rule 3-2(c), a substantial part of the events giving rise to the claims brought in this Complaint occurred in San Mateo County, California. Consequently, assignment of this action to San Francisco or Oakland Division is appropriate.

PARTIES

Gabriele Willis

13. Plaintiff Gabriele Willis is an adult citizen of the state of California who resides in El Cajon, California. Ms. Willis has had an active Facebook account since approximately 2007. She has used her iPhone to access the Facebook app since approximately 2008. Her device has run on iOS version 14.5 or later since approximately May 2021.

14. Ms. Willis did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

15. Using the systematic process described below, Meta tracked and intercepted Ms. Willis's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Willis reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Shelby Cooper

16. Plaintiff Shelby Cooper is an adult citizen of the state of California who resides in Riverside, California. Ms. Cooper has had an active Facebook account since approximately 2004. She has used her iPhone to access the Facebook app since approximately 2008. Her device has run on iOS version 14.5 or later since approximately April 2021.

17. Ms. Cooper did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

18. Using the systematic process described below, Meta tracked and intercepted Ms. Cooper's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Cooper reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Rama Kolesnikow

19. Plaintiff Rama Kolesnikow is an adult citizen of the state of California who resides in Culver City, California. Mr. Kolesnikow has had an active Facebook account since May 2008. He has used his iPhone to access the Facebook app since approximately late 2008 to early 2009. His device has run on iOS version 14.5 or later since approximately April 2021.

20. Mr. Kolesnikow did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

21. Using the systematic process described below, Meta tracked and intercepted Mr. Kolesnikow's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Kolesnikow reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Lisa Bush

22. Plaintiff Lisa Bush is an adult citizen of the state of Florida who resides in Sebastian, Florida. Ms. Bush has had an active Facebook account since 2008. She has used her iPhone to access the Facebook app since December 2021. Her device has run on iOS version 14.5 or later since approximately December 2021.

23. Ms. Bush did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

24. Using the systematic process described below, Meta tracked and intercepted Ms. Bush's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Bush reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

David Alzate

25. Plaintiff David Alzate is an adult citizen of the state of Florida who resides in Miami, Florida. Mr. Alzate has had an active Facebook account since approximately 2007. He has used his

iPhone to access the Facebook app since 2012. His device has run on iOS version 14.5 or later since April 2021.

26. Mr. Alzate did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

27. Using the systematic process described below, Meta tracked and intercepted Mr. Alzate's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Alzate reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Mark Letoski

28. Plaintiff Mark Letoski is an adult citizen of the state of Illinois who resides in Chicago, Illinois. Mr. Letoski has had an active Facebook account since approximately December 2005. He has used his iPhone to access the Facebook app since approximately 2008. His device has run on iOS version 14.5 or later since approximately April 2021.

29. Mr. Letoski did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

30. Using the systematic process described below, Meta tracked and intercepted Mr. Letoski's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Letoski reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Louis Green

31. Plaintiff Louis Green is an adult citizen of the state of Illinois who resides in Hazel Crest, Illinois. Mr. Green has had an active Facebook account since approximately March 2010. He has used his iPhone to access the Facebook app since approximately March 2010. His device has run on iOS version 14.5 or later since approximately April 2021.

32. Mr. Green did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

33. Using the systematic process described below, Meta tracked and intercepted Mr. Green's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Green reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Ed Rennie

34. Plaintiff Ed Rennie is an adult citizen of the state of Massachusetts who resides Salem, Massachusetts. Mr. Rennie has had an active Facebook account since approximately 2009. He has used his iPhone to access the Facebook app since approximately 2011. His device has run on iOS version 14.5 or later since approximately April 2021.

35. Mr. Rennie did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

36. Using the systematic process described below, Meta tracked and intercepted Mr. Rennie's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Rennie reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable

information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Teia Pittman

37. Plaintiff Teia Pittman is an adult citizen of the state of Maryland who resides in Baltimore, Maryland. Ms. Pittman has had an active Facebook account since approximately 2008. She has used her iPhone to access the Facebook app since approximately 2011. Her device has run on iOS version 14.5 or later since April 2021.

38. Ms. Pittman did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

39. Using the systematic process described below, Meta tracked and intercepted Ms. Pittman's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Pittman reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Raven Johnson

40. Plaintiff Raven Johnson is an adult citizen of the state of Missouri who resides in Cape Girardeau, Missouri. Ms. Johnson has had an active Facebook account since approximately 2010. She has used her iPhone to access the Facebook app since approximately 2012. Her device has run on iOS version 14.5 or later since April 2021.

41. Ms. Johnson did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

42. Using the systematic process described below, Meta tracked and intercepted Ms. Johnson's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Johnson reasonably expected

that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Chanel Robinson

43. Plaintiff Chanel Robinson is an adult citizen of the state of Pennsylvania who resides in Philadelphia, Pennsylvania. Ms. Robinson has had an active Facebook account since approximately 2009. She has used her iPhone to access the Facebook app since 2012. Her device has run on iOS version 14.5 or later since April 2021.

44. Ms. Robinson did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

45. Using the systematic process described below, Meta tracked and intercepted Ms. Robinson's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Robinson reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Kevin Zenstein

46. Plaintiff Kevin Zenstein is an adult citizen of the state of Pennsylvania who resides in Lafayette Hill, Pennsylvania. Mr. Zenstein has had an active Facebook account since approximately 2013. He has used his iPhone to access the Facebook app since approximately 2013. His device has run on iOS version 14.5 or later since approximately April 2021.

47. Mr. Zenstein did not consent to Facebook tracking his activity. He configured the settings on his iPhone to not allow the Facebook app to track him.

48. Using the systematic process described below, Meta tracked and intercepted Mr. Zenstein's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without his knowledge or consent. Mr. Zenstein reasonably expected that his communications with third-party websites were confidential, solely between himself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Mary Thew

49. Plaintiff Mary Thew is an adult citizen of the state of Washington who resides in Deer Park, Washington. Ms. Thew has had an active Facebook account since June 2016. She has used her iPhone to access the Facebook app since June 2016. Her device has run on iOS version 14.5 or later since April 2021.

50. Ms. Thew did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

51. Using the systematic process described below, Meta tracked and intercepted Ms. Thew's specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Thew reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Lisa Evans

52. Plaintiff Lisa Evans is an adult citizen of the state of Washington who resides in Mead, Washington. Ms. Evans has had an active Facebook account since 2007. She has used her iPhone to access the Facebook app since 2010. Her device has run on iOS version 14.5 or later since April 2021.

53. Ms. Evans did not consent to Facebook tracking her activity. She configured the settings on her iPhone to not allow the Facebook app to track her.

54. Using the systematic process described below, Meta tracked and intercepted Ms. Evans' specific electronic activity and private communications with third-party websites opened within Facebook's in-app browser without her knowledge or consent. Ms. Evans reasonably expected that her communications with third-party websites were confidential, solely between herself and those websites, and that such communications—which include text entries, passwords, personally identifiable information, and other sensitive, confidential and private information—would not be intercepted or tracked by Meta.

Meta Platforms, Inc.

55. Defendant Meta Platforms, Inc., d/b/a as Meta, formerly known as Facebook, Inc., is a Delaware corporation headquartered in Menlo Park, California.

FACTUAL ALLEGATIONS

A. Meta's business model is predicated on accumulating user data and selling it to generate advertising revenue

56. Meta's core business depends on collecting revenue by targeting ads to its users and selling advertising space on its social media and messaging platforms. Meta earns revenue by selling digital ads to other businesses seeking to promote their goods or services to Facebook users on a targeted basis. Hence, though Meta does not require Facebook members to pay a monetary subscription fee, membership is far from free. Meta profits by collecting and analyzing its users' personal information and using it to sell more precisely targeted ads.

57. On Facebook, advertisers can reach an audience of well over a billion people. Facebook averaged approximately 196 to 197 million daily active users in the United States and Canada during the first three quarters of 2022. Nearly all these users accessed Facebook on their mobile devices.

58. Meta's informational advantage and vast user base allow marketers to target advertisements to specific types of people based on characteristics such as age, gender, location, preferences, and behaviors. Meta maximizes its profits by targeting ads to people using algorithms that

indicate they may take interest in a certain advertised product or service. Meta's profits thus depend on connecting advertisers with its massive repository of personal data on the users of its platforms. To this end, Meta collects extensive data about its users, attributes users' data and browsing activity to their individual accounts, continuously aggregates and analyzes this data using advanced algorithms, and deploys the data to sell targeted advertising services.

59. The personal information Meta collects has economic value. An older study valued users' web-browsing histories at $52 per year. The Organization for Economic Cooperation and Development estimated the prices for various individual data points: $0.50 for an address, $2 for birthdate, $8 for a Social Security number, $3 for a driver's license number, and $35 for a military record. More recent estimates suggest the value of personal data continues to be high: a personal email can be worth $89, a complete health care record is valued at around $250, and a hacked Facebook account can sell for $65 on the dark web. Similarly, a 2019 report found that data generated from an adult is worth roughly $35 per month.

60. Between 2009 and 2021 Meta's annual advertising revenues grew exponentially. In 2021 Meta took in over $114 billion in advertising revenue, which accounted for 97% of Meta's total revenue in 2021, an approximately 37% year-over-year increase of around $31 billion.

B. Meta's tracking of users before Apple's iOS 14.5 software update

61. In late 2020 Apple announced that its iOS 14.5 software update would change how its Apple Devices handle users' privacy preferences, requiring apps to obtain users' affirmative consent to being tracked before tracking them. Apple stated that these changes were intended to provide users of Apple products with greater privacy and control over their mobile app data.

62. Before the iOS 14.5 software update, the default settings on Apple Devices required users to opt out of being tracked by apps. As such, app owners and developers could track users by default, unless the user changed their settings. Therefore, apps, including Facebook, on most Apple Devices could access user-level data and the Identifier for Advertising ("IDFA") without the device owner's consent.

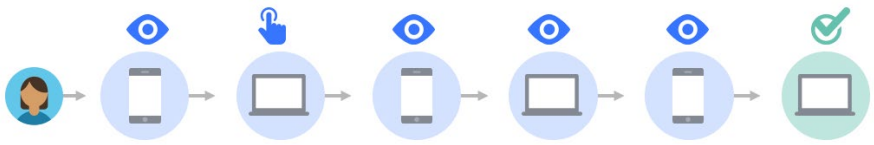
63. The IDFA is a random device identifier assigned by Apple to a user's Apple Device that allows the app to recognize that specific device and track the user's activity across third-party websites. IDFAs enable precise targeting and tracking of users within apps on Apple Devices. Using the IDFA,

information collected through an app or website can be connected to information about the user gathered from other online locations.

64. Before Apple's iOS 14.5 software update, Meta used a tool called Facebook Attribution that enabled advertisers to measure and understand the impact of their ads across multiple publishers, channels, and devices. This tool helped advertisers understand the true value of their ads and assess which were most effective. But without the ability to collect IDFAs and monitor users' activity across third-party websites, Meta cannot see how users are engaging with ads on the Facebook app and track them as they progress through various "touchpoints" on different devices. Such attribution is critical to digital marketing.

65. Meta describes attribution as "the process of assigning credit to touchpoints along a consumer's conversion path. By understanding which of your ads should get credit for leading a consumer to take an action you wanted, such as making a purchase, you can better measure the effectiveness of your ads and make decisions for future planning and optimization." As Meta further explains:

> [L]et's say someone saw your ads while browsing the Facebook app on their mobile phone, on a website they visited while on their work computer, and on a search engine while on their home computer. If the last ad that this person clicked on before making their purchase was the ad on the search engine from their home computer, it can be tempting to think that this search engine ad should get all the credit for making the sale happen, even though all of the other ads contributed to building awareness and consideration.
>
> Each of these steps leading up to the conversion are called touchpoints, which include any of a consumer's interactions with an ad. They make up a consumer's conversion path, which may look something like this:



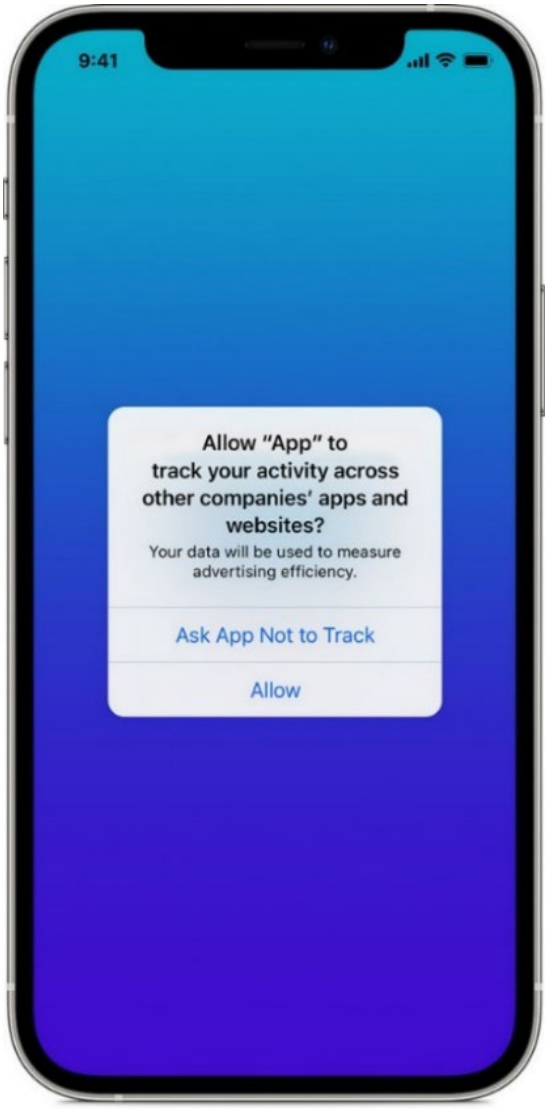
> For example, the first touchpoint may introduce someone to a brand or product, the middle touchpoints may help increase their consideration of the product and the last touchpoint may lead them to take the action of converting. Attribution combines the data from the touchpoints in a consumer's conversion path with the model you choose to apply to this data to understand which touchpoints should get credit for the conversion.

C. Apple's iOS 14.5 update

66. Apple's iOS 14.5 software update, introduced in April 2021, added App Tracking Transparency ("ATT"). ATT converted the "opt out of tracking" framework to an "opt-in" regime. Hence, with iOS 14.5 and later, apps including Facebook must first obtain a user's permission before accessing their IDFA and tracking their activity across third-party websites. Reasonable consumers understand that by choosing not to "opt in" to tracking, they are denying the app permission to track their keystrokes and other activities as they navigate from the Facebook app to a third-party website.

67. For companies like Meta that generate revenue by selling digital ads, Apple's iOS 14.5 software update made it much harder to precisely target ads using existing algorithms and to attribute a user's online purchase to a specific ad or ad campaign. Because Meta monetizes online activity by converting it to information useful to advertisers, the sudden inability to track consumer browsing activities threatened Meta's bottom line. Meta continues to confront this challenge as each subsequent iteration of Apple's iOS, up to and including the current version, iOS 16.3, supports the same ATT functionality.

68. With ATT, Apple Device users see a pop-up message when they first launch an app that is generated directly from the app that seeks to track their activity. As shown in Figure 1 below, the bolded message on top asks: "Allow 'App' to track your activity across other companies' apps and websites?" Below, in blue text, the user is prompted to tap either "Ask App Not to Track" or "Allow." The user must make a selection or cannot proceed into the app; the choice is a mandatory step in the navigation.



(Figure 1 – Image of the pop-up message that appears on Apple devices)

69. If a user selects "Ask App Not to Track," the app is not able to access the IDFA or track the user's activity using other information that identifies the user or their device. If a user selects "Allow," the app is able to access the IDFA and may track the user in the manner it did prior to iOS 14.5 and ATT. Accordingly, Meta is aware of the user's response to this prompt, as this decision dictates whether Meta can access the IDFA or gather data as it traditionally has.

70. Apple Device users also can configure their settings to *automatically* decline *every* app's request to track their activity, by turning off the "Allow Apps to Request to Track" option in the device's privacy settings. When this option is de-selected, no message prompt appears when an app requests to track the user across third-party websites; the technology treats any such request as if the user had selected

"Ask App Not to Track," thereby preventing IDFA access and other tracking.

71. Thus, Apple Device users can indicate whether they consent to being tracked in one of two ways: (1) via the tracking request pop-up message received from a particular app; or (2) by configuring their setting to automatically reject all tracking requests. Accordingly, tracking by an app after the iOS 14.5 software update requires the user's express permission. Absent such permission, tracking by an app overrides and disregards the user's denial of consent.

72. Apple's policy shift fundamentally altered—and enhanced—the degree of control the individual user has over the information they share with the apps on their Apple Devices. By requiring apps to obtain permission *before* tracking users, Apple changed its mobile device privacy framework so as to obtain clear, advance user consent or declination to being tracked. Users were thus empowered to decide whether they want to be tracked by the Facebook app at all, putting the onus on Meta to obtain users' affirmative consent.

73. When presented with this privacy choice, Plaintiffs and Class Member explicitly declined to be tracked by Meta, either by (a) tapping "Ask App Not to Track" when prompted by the pop-up message from the Facebook app, or (b) configuring their Apple Device settings to automatically decline requests to track their activity across websites. Their clearly expressed privacy preference, therefore, was *not* to be tracked by Meta when navigating to third-party websites from the Facebook app.

74. Through the ATT framework, Meta knows whether users have consented to tracking by the Facebook app. Without this consent, Meta is not permitted to link together user or device data (a) collected from the Facebook app with (b) such data collected from third-party websites—a linkage critical for targeted advertising and related analytics. Thus, in addition to being a mandatory element of the ATT framework, whether Apple Device users permit tracking is bound up with Meta's digital advertising business. Yet despite knowing that Plaintiffs and Class Members did not consent to being tracked by the Facebook app, Meta tracked them anyway.

D. Meta's lost profits and P.R. effort in response to Apple's iOS 14.5 update

75. As noted above, following Apple's privacy policy change and implementation of ATT, Meta's digital advertising revenue sharply declined: "According to [Meta], empowering Apple's users to opt out of tracking cost the company $10,000,000,000 in the first year, with more losses to come after

that," according to the Electronic Frontier Foundation. In Q2 2022, Meta's ad revenue decreased by 1% compared to the same period in 2021, and in Q3 2022, Meta's revenue decreased by 4% compared to the same period the year before.

76. Meta attributed the large declines in part to Apple's changes to its iOS operating system in April 2021. In its Q2 2022 Form 10-Q quarterly report, Meta stated, "[o]ur advertising revenue continues to be adversely affected by reduced marketer spending as a result of limitations on our ad targeting and measurement tools arising from changes to the iOS operating system beginning in 2021." Meta acknowledged that Apple's "changes to iOS . . . limit our ability to target and measure ads effectively." In its Q3 2022 Form 10-Q quarterly report, Meta stated that "in 2021, Apple made certain changes to its products and data use policies in connection with changes to its iOS operating system that reduce our and other iOS developers' ability to target and measure advertising, which has negatively impacted, and we expect will continue to negatively impact, the size of the budgets marketers are willing to commit to us and other advertising platforms."

77. Recognizing that most iOS users would not consent to tracking if given the choice, Meta vehemently criticized and opposed Apple's privacy shift and attempted to sway public opinion against it. As reported by CNN, after Apple's announcement of iOS 14.5, Meta began "waging a public relations effort to attack Apple ahead of new iOS data privacy changes that would make it harder for advertisers to track users, in a possible sign of just how much the social network views the move as a threat to its core business." Meta held press conferences and ran advertisements critical of Apple's decision to require affirmative user consent to being tracked. In ads in The New York Times, Wall Street Journal and Washington Post, Facebook disparaged Apple's upcoming requirement for users to give explicit permission for apps to track them, arguing the move would impair targeted advertising and therefore could be "devastating" to millions of small business advertisers. Meta-owned WhatsApp also joined in, "criticiz[ing] Apple over its move to display a summary of an app's privacy practices before a user downloads it from the App Store, almost like a nutrition label for data collection."

78. Apple responded in part, "We believe that this is a simple matter of standing up for our users. Users should know when their data is being collected and shared across other apps and websites—and they should have the choice to allow that or not." Apple further noted that "App Tracking

Transparency in iOS 14 does not require Facebook to change its approach to tracking users and creating targeted advertising, it simply requires they give users a choice."

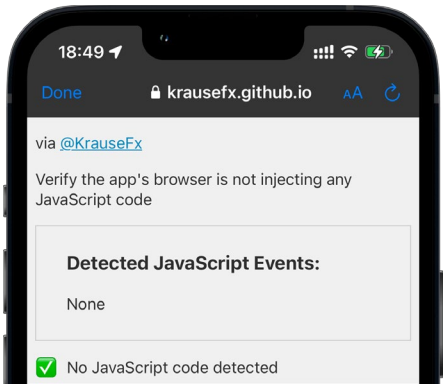
79. As of May 2021, shortly after Apple introduced iOS 14.5, 96% of Apple users in the United States had *not* consented to being tracked by apps on their iPhone. In response Meta began showing its users a screen that described its view of the consequences of iOS 14.5, including potential long-term harm to Meta's ability to provide apps and software. Through these and related communications strategies, contemporaneous reports noted, Meta was "threatening that users will need to pay for their services. But only if users don't allow [Meta] to track them from app to app after installing iOS 14.5."

80. Meta could not stop the iOS 14.5 change and ATT framework from going into effect. To reverse the ensuing steep drop in revenue, Meta covertly deployed hidden code into third-party websites via its in-app browser to track and monitor its users—and maintain access to their data—in contravention of their stated preference not to be tracked by the Facebook app.

E. How Meta secretly overrides users' privacy settings

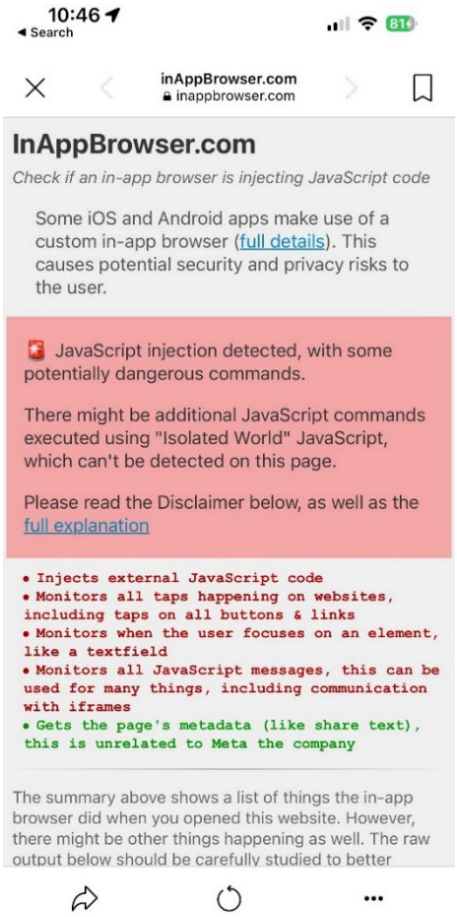
81. By injecting code into third-party websites, Meta is able to track users and intercept data that would otherwise be unavailable to it. When a Meta user clicks on a link to an external website from the Facebook app (e.g., from a friend's post on their profile), Meta *automatically* reroutes the user to its own in-app web browser instead of the users' built-in web browser (such as Apple's Safari app that is preloaded onto iPhones). When this occurs, Meta injects a type of programming code known as JavaScript into third-party websites so that it can track users' activities on those websites. Third-party websites are rendered *inside* the app—enabling Meta to monitor everything happening on external websites, without consent from the user or from the website itself.

82. A computer science expert, Felix Krause, helped develop www.InAppBrowser.com, a website that allows users to detect whether a particular in-app browser is injecting code into third-party websites. Figure 2 below shows what happens when a user clicks on a web link they received in the Telegram app, a messaging platform that does not inject JavaScript into third-party websites, but which openly prompts users to use Telegram's own in-app browser instead of a default browser:



(*Figure 2*) Hence, as demonstrated by the image above, not all in-app browsers disregard users' privacy or override their devices' privacy settings. Telegram, in other words, does not track users' activity on or communications with third-party web pages.

83. Compare the Telegram image in Figure 2 above with the image shown in Figure 3 below, displaying what happens when a user clicks on a web link in the iOS Facebook app:



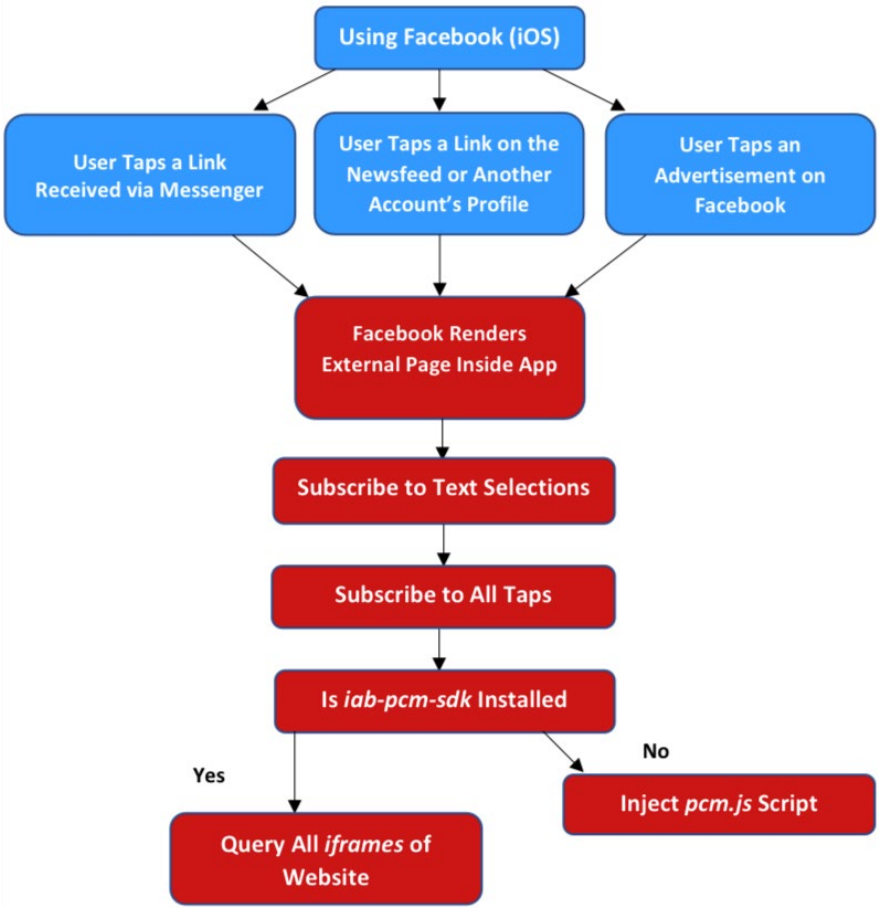
(*Figure 3*) Thus, when the same HTML file (website) is opened from the iOS Facebook app, www.InAppBrowser.com detects and identifies several different JavaScript events.

84. Krause's report, entitled "*iOS Privacy: Instagram and Facebook can Track Anything you do on any Website in their In-App Browser*," describes how Meta uses JavaScript to alter websites and override its users' default privacy settings by sending users to Facebook's in-app browser instead of their default web browser.

85. Meta's practice of injecting its JavaScript code into the code of third-party websites is similar to actions taken by malicious actors seeking to intercept confidential information communicated to a website. As one data security company described:

> **What is a JavaScript Injection Attack?**
>
> A JavaScript injection attack is a type of attack in which a threat actor injects malicious code directly into the client-side JavaScript. This allows the threat actor to manipulate the website or web application and collect sensitive data, such as personally identifiable information (PII) or payment information.

86. When the Facebook app injects Meta's JavaScript code ("pcm.js") into a third-party website accessed from within Facebook's in-app browser, it creates a bridge to communicate between the Facebook app and the third-party website. This allows Meta to intercept and record users' interactions and communications with third parties, providing data that Meta analyzes and uses to boost its advertising revenue. As illustrated in Figure 4 below, this systematic process occurs whenever a user clicks on a link they received in their inbox (through the private messaging feature), or when they click on a link displayed on their "news feed" or on another Facebook account's "profile" or post, or when they tap a link within Facebook that is a digital ad.



(*Figure 4*) The image above depicts the systematic manner in which Meta injects its JavaScript code into third-party webpages for the purpose of intercepting, tracking, monitoring, and collecting data about its users' interactions with those webpages.

87. After causing the third-party website to be rendered in Facebook's in-app browser, Meta adds JavaScript "event listeners" to the third-party website. As the name suggests, "event listeners" are pieces of JavaScript code that "listen" and trigger every time an "event" occurs. For the Facebook in-app browser, Meta has implemented JavaScript event listeners that listen for (or "subscribe to"): any tap on a button or link; any time a user focuses on an element (such as selecting a text field); and all JavaScript messages.

88. When users engage with any of these "events" on the third-party website rendered within Facebook's in-app browser, an event listener contemporaneously captures and transmits the information to the Facebook app. Hence the event listeners operate like a keystroke logger, allowing Meta to acquire,

in real time, information a user transmits to a third-party website in real time, before that information is electronically stored. In this way, Meta accesses and intercepts this information while it is in transit to the third-party site.

89. These event listeners are critical to Meta's ability to intercept, view, monitor, and record all user interactions with third parties—every button and link users tap, text selections, screenshots, form inputs (including passwords, addresses, and payment card numbers), personally identifiable information, protected health details, and other private and confidential communications and data. In the context of an online purchase, Facebook's in-app browser collects and records all details of the purchase, including the item purchased; name and address of purchaser; their telephone number, credit card or bank information, usernames, passwords and birthdate; and the purchase price. Similarly, Facebook's in-app browser acquires and records details about certain users' physical and mental health when they click on a link to a medical provider's website. Once there, HIPAA-protected health information provided by the user also can be intercepted and captured by Meta.

90. At no point while communicating with a third-party website did Plaintiffs or Class Members intend to transmit any information to Meta or the Facebook app. On the contrary, all Plaintiffs and Class Members expressly denied Meta permission to monitor their online activity.

91. Meta's surreptitious conduct precludes a reasonable user from knowing the Facebook app receives any information once they tap a link to a third-party website.

92. Additionally, Meta's pcm.js scans the third-party website rendered within Facebook's in-app browser to detect whether the Meta Pixel is present on the website. The Meta Pixel is a snippet of programming code that, once installed on a website, allows website owners to track visitor actions to target products and services to those visitors on Facebook. Meta tells website owners that the Meta Pixel allows it "to match your website visitors to their respective Facebook User accounts."

93. If the Meta Pixel is present on the third-party website, Meta's JavaScript code will exfiltrate the Meta Pixel data from the website to the Facebook app in real time. This data includes personally identifiable information and information about the content users viewed on the third-party website. For example, if a user on a financial services website interacts with a button corresponding to their credit score, that personal information would be included in the data that Meta acquires.

94. Meta is therefore able to surveil and extract details about users' texting, selections, and other communications with third-party websites. Krause further described technical elements of this process:

> [Event listeners], in combination with listening to screenshots, gives Meta full insight over what specific piece of information was selected & shared. The [Meta] app checks if there is an element with the ID iab-pcm-sdk: According to this tweet, the iab likely refers to "In App Browser". If no element with the ID iab-pcm-sdk was found, [Meta] creates a new script element, sets its source to https://connect.facebook.net/en_US/pcm.js. It then finds the first script element on [the] website to insert the pcm JavaScript file right before. [Meta] also queries for iframes on [the] website.

95. For users of iOS 14.5 or later, Meta's tracking occurs even if those users—like all Plaintiffs and Class Members—*declined* to consent by tapping "Ask App Not to Track" or their device settings were configured to decline all requests to track. If a user accessed the same third-party website directly through Apple's Safari web browser, instead of Facebook's in-app browser, Safari would actively block and prevent Meta's ability to intercept and track the user's activity on the third-party website. But, through the mechanisms detailed above, Meta tracks this same activity when the user engages in activity through Facebook's in-app browser.

96. Meta knowingly tracks users across the web in a manner that circumvents users' privacy preferences and ATT settings on their Apple devices. Further, the technical nature and complexity of Meta's conduct, in sending users to its own undisclosed in-app browser that is invisibly configured to intercept and redirect users' communications to Meta, makes it impossible for ordinary users to realize what Meta is doing.

F. Meta's conduct harmed Plaintiffs and Class Members

97. Meta does not inform Facebook users that clicking on links to third-party websites from within Facebook will automatically send the user to Facebook's in-app browser, as opposed to the user's default web browser, or that Meta will monitor the user's activity and communications while browsing on those sites. Because nothing alerts users to these facts, they are unaware of the tracking. Users freely engage with these sites, sharing all manner of personal facts and preferences, without having reason to suspect they are being tracked or are still within Facebook's app.

98. Meta fails to disclose the consequences of browsing, navigating, and communicating with third-party websites from within Facebook's in-app browser—namely, that doing so may override the privacy settings and preferences of users intended to block and prevent tracking. Meta also conceals that it injects JavaScript that alters external third-party websites so that it can intercept, track, and record data it otherwise could not access. There was never any pop-up window or other conspicuous notice to users regarding Meta's tracking practice. The relevant "Off-Facebook activity" settings tab within the Facebook app did not disclose the practice. At no point did Meta fairly or reasonably disclose to users its practice of intercepting, monitoring, and selling information gleaned from their online activities and communications even after they declined consent to being tracked.

99. Even users who may realize they are visiting websites from within Facebook's in-app browser are not informed that the browser ignores, rejects, and overrides their pop-up response or privacy settings and enables Meta to track, intercept, and monitor their activities on third-party websites. A reasonable consumer has no way of detecting Meta's JavaScript injection; a website viewed within Facebook's in-app browser functions no differently than otherwise. Nor would a reasonable consumer expect Meta to disregard and override their clearly communicated refusal to be tracked by embedding JavaScript code on the third-party websites accessed through the Facebook app.

100. Most users of Apple Devices running iOS 14.5 and above also reasonably expect that their communications with external third-party websites are not being intercepted and tracked because Apple's default browser for its devices, Safari, disables and blocks third-party cookies. Meta does not inform users that its in-app browser differs from Safari and other browsers regarding such privacy settings.

101. Plaintiffs reasonably believed that their communications and interactions with third-party websites were solely with those sites. Had Plaintiffs known that Meta could and would use its in-app browser to nullify Plaintiffs' ATT settings and other privacy choices, Plaintiffs would have avoided navigating to third-party websites from within Facebook. Instead, they would have copied and pasted hyperlinks into their standard browser to avoid being tracked, and ensured that their communications with third-party websites were made outside of any Meta platform, particularly when the communications involved sensitive or other personally identifiable information, such as private health information.

G. Meta has a track record of pursuing profit at the expense of its users' privacy

102. Meta's conduct set forth above follows from its business model, which depends on access to detailed information about its users. This model has led Meta to monitor and surveil its users through use of plug-ins, cookies, Facebook Beacon, the Facebook Like Button, Facebook Pixel, and other data mining tactics. Meta has consistently shared its users' private messages and the details relating to their personal contacts without those users' consent. From 2010 to 2018 Facebook allowed more than 150 third parties, including Amazon and Microsoft, to access this private information. In 2019, Facebook agreed to pay a $5 billion penalty and submit to new restrictions and a modified corporate structure to settle Federal Trade Commission charges that Facebook violated a 2012 FTC order by deceiving users about their ability to control the privacy of their personal information.

103. The U.S. Department of Justice likewise has alleged that Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences. Among other misleading practices, Facebook removed its disclosure on its main "Privacy Settings" page that information shared with a user's Facebook friends could also be shared with the apps used by those friends, while continuing to share data from users' Facebook friends with third-party developers. Similarly, Facebook launched features that claimed to help users better manage their privacy settings in 2012 and 2014 but failed to disclose that even the most restrictive sharing settings would not cause Facebook to stop sharing user information with apps used by the user's Facebook friends, unless the user also opted out of such sharing on a separate settings page. In April 2014, Facebook announced that it would stop allowing third-party developers to collect data about the friends of app users, but separately told developers that they could collect this data until April 2015 if they already had an existing app on the platform. And between November 2015 and March 2018 Facebook told users it would collect their phone numbers to enable a security feature, failing to tell them it also used those numbers for advertising purposes.

CLASS ACTION ALLEGATIONS

104. Plaintiffs bring this lawsuit under Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3) and/or (c)(4) as representatives of the following Class and constituent Subclasses (collectively, the "Class"):

Class: All persons in the United States with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher, and (ii) did not allow the Facebook app to track them.

California Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in California, and (ii) did not allow the Facebook app to track them.

Florida Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Florida, and (ii) did not allow the Facebook app to track them.

Illinois Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Illinois, and (ii) did not allow the Facebook app to track them.

Maryland Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Maryland, and (ii) did not allow the Facebook app to track them.

Massachusetts Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Massachusetts, and (ii) did not allow the Facebook app to track them.

Missouri Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Missouri, and (ii) did not allow the Facebook app to track them.

Pennsylvania Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Pennsylvania, and (ii) did not allow the Facebook app to track them.

Washington Subclass: All persons with active Facebook accounts who (i) visited a third-party external website on Facebook's in-app browser while using an Apple Device running iOS 14.5 or higher in Washington, and (ii) did not allow the Facebook app to track them.

105. Excluded from the Class are all Facebook users who tapped "Allow" on Apple's "Allow App to Track?" pop-up window or configured their Apple Device settings to permit apps to track their activity. Also excluded from the Class are Meta and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them has a controlling interest, as well as all persons employed by counsel in this action and any judge to whom this case is assigned, his or her spouse and immediate family members, and members of the judge's staff.

106. The Class Period extends from the date that Meta began implementing the practices described in the Complaint to the date of entry of judgment. Plaintiffs may modify the Class and Subclass definitions or propose additional subclasses as appropriate based on further investigation and discovery.

107. Numerosity. The members of the Class are so numerous that joinder of all members would be impracticable. While the number of Class Members is unknown to Plaintiffs at this time, it is estimated to number in the millions. The identity of Class Members is readily ascertainable from Meta's records.

108. Typicality. Plaintiffs' claims are typical of the claims of the Class because Plaintiffs used Meta's platforms to view third-party websites that were embedded as URLs within the respective Meta applications, and all Class Members were subjected to Meta's wrongful and invasive tracking practices.

109. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the Class Members. Plaintiffs' interests are coincident with, and not antagonistic to, those of the Class Members. Plaintiffs are represented by attorneys experienced in the prosecution of class action litigation, including digital privacy protection litigation, who will vigorously prosecute this action for the Class.

110. Common Questions of Law and Fact Predominate. Questions of law and fact common to the Class Members predominate over questions that may affect only individual Class Members because Meta has acted on grounds generally applicable to the Class. The following questions of law and fact are common to the Class and predominate over any individual issues:

a. Whether Meta intentionally tapped the lines of electronic communication between Class Members and third-party websites they visited;

b. Whether Meta intentionally intercepted the private information of Class Members in transit without their consent;

c. Whether Facebook's in-app web browser secretly monitored and recorded Class Members' private communications and personally identifiable information;

d. Whether Meta violated state and federal laws by tracking its users' online activities and intercepting their communications when they visited third-party websites, even when they expressly indicated that they did not wish to be tracked;

e. Whether Class Members have a reasonable expectation of privacy with respect to such information;

f. Whether Meta's invasion of Class Members' privacy rights is highly offensive to a reasonable person;

g. Whether Meta's statements and omissions misled Class Members as to the level of control they had over their private communications derived from activity on the Facebook app;

h. Whether Meta was unjustly enriched as a result of its wrongful and invasive practices; and

i. Whether Class Members are entitled to damages, restitution and/or injunctive relief in view of Meta's conduct.

111. Superiority. A class action will permit numerous similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication

of evidence, effort, or expense. A class action will provide injured persons a method for obtaining redress on claims that could not practicably be pursued individually. Plaintiffs know of no manageability or other issue that would preclude maintenance of this case as a class action.

112. Class certification is also appropriate under Rules 23(b)(1), (b)(2), and/or (c)(4) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Meta;
- The prosecution of separate actions by individual Class Members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;
- Meta has acted or refused to act on grounds generally applicable to the Class, making injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole; and
- The claims of Class Members are comprised of common issues whose resolution in a class trial would materially advance this litigation.

TOLLING OF THE STATUTES OF LIMITATIONS

113. All applicable statute(s) of limitations have been tolled by Meta's knowing and active concealment and denial of the facts alleged herein. Plaintiffs and Class Members could not have reasonably discovered Meta's practice of tracking and intercepting their activities and communications while they have an in-app browser open, even after they declined to consent to being tracked, until shortly before this class action litigation commenced.

114. Meta was and remains under a continuing duty to disclose to Plaintiffs and Class Members its practice of tracking and intercepting their activities and communications while they have an in-app browser open. As a result of the active concealment by Meta, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

FIRST CLAIM FOR RELIEF

VIOLATION OF THE WIRETAP ACT
18 U.S.C. § 2510 *et seq*.
(On Behalf of the Class)

115. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class.

116. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986 ("ECPA"), prohibits the intentional interception of any wire, oral, or electronic communication.

117. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

118. **Electronic Communications.** The communications between Plaintiffs and Class Members and third-party websites are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

119. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

120. **Interception.** The ECPA defines interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

121. **Electronic, Mechanical, or Other Device.** The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

(a) Plaintiffs' and Class Members' browsers;

(b) Plaintiffs' and Class Members' Apple Devices;

(c) Defendant's mobile applications including the Facebook app;

(d) Defendant's in-app browser;

(e) Defendant's electronic servers; and

(f) The code deployed by Defendant to circumvent users' privacy controls and transmit their communications to Defendant.

122. Without Plaintiffs', Class Members', or third-party websites' knowledge or consent, Meta intercepted the contents of their electronic communications when they navigated from Facebook to third-party websites.

123. Meta intentionally used technology, including the JavaScript code it injected into third-party websites, as a means of intercepting and acquiring the contents of Plaintiffs' and Class Members' electronic communications, in violation of the Wiretap Act.

124. Meta intentionally intercepted Plaintiffs' and Class Members' information in transit. Meta intercepted Plaintiff's and Class Members' website communications, whenever they used Facebook's in-app browser to communicate with third-party websites, using the JavaScript code inserted by Meta, including every click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications—which comprise the transfer of signs, signals, writing, images, sounds, data, and/or intelligence transmitted in whole or in party by wire, radio, electromagnetic, photoelectric, or photo-optical system—constitute "electronic communications" under the Wiretap Act and were contemporaneously copied by Meta in real time.

125. The personal information was content as defined by the Wiretap Act as it involves the substance and import of Plaintiffs' communications with third-party websites and not simply routine identifiers or metadata. Meta configured and implemented code to surreptitiously capture user information such as keystrokes, search queries, and information entered into forms or text boxes.

126. Plaintiffs and Class Members were not aware that Meta was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites. Plaintiffs and Class Members did not consent to Meta's tracking and collection of their personal communications, and in fact they affirmatively opted out of such tracking on their Apple Devices.

Additionally, the nature of the tracking and collection of information at issue goes beyond what a reasonable consumer would anticipate when using the internet or mobile applications.

127. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

128. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

129. Plaintiffs and Class Members are persons whose electronic communications were intercepted within the meaning of Section 2520. As such, they are entitled to preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual damages, punitive damages, and reasonable attorneys' fees and costs of suit.

SECOND CLAIM FOR RELIEF

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
18 U.S.C. § 1030 *et seq.* ("CFAA")
(On Behalf of the Class)

130. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class.

131. The Consumer Fraud and Abuse Act establishes a private cause of action against a person who "knowingly accessed a computer without authorization or exceeding authorized access," and whose prohibited access results in damage or loss in excess of $5,000. 18 U.S.C. § 1030(g) (referencing § 1030(c)(4)(A)(i)(I)); *see also* § 1030(a).

132. The CFAA establishes liability against whomever:

(a) "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer" (§ 1030(a)(5)(A));

(b) "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" (§ 1030(a)(5)(B)); or

(c) "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss" (§ 1030(a)(5)(C)).

133. The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]" 18 U.S.C. § 1030(e)(1).

134. A "protected computer" is defined, in relevant part, as a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B).

135. "[E]xceeds authorized access" means "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

136. "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11).

137. Damage means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

138. Plaintiffs' and Class Members' Apple Devices are "computers" under the CFAA by virtue of their data processing and storage functions and their operation in conjunction with other similar devices.

139. Plaintiffs' and Class Members' Apple Devices are "protected computers" under the CFAA because, at all relevant times, they are and were used in and affect interstate and foreign commerce and communication, including through contact and communication with remote servers and through personal and business usages that affect interstate and foreign commerce.

140. Defendant exceeded, and continues to exceed, its authorized access to Plaintiffs' and Class Members' protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2).

141. Defendant knowingly and intentionally exceeded its authorized access to Plaintiffs' and Class Members' Apple Devices. Plaintiffs and Class Members did not consent to be tracked by the Facebook app across third-party websites and configured their devices to reject such requests.

142. By exceeding its authorized access, Defendant obtained Plaintiffs' and Class Members' private and personally identifiable data and communications—including their clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications. Defendant's injection of code into third-party websites rendered within Facebook's in-app browser allowed it to access information that it could not otherwise obtain.

143. By injecting code into third-party websites rendered within Facebook's in-app browser, Defendant knowingly caused the transmission of "a program, information, code, or command … to a protected computer" and, as a result of that conduct, intentionally caused damage in violation of 18 U.S.C. § 1030(a)(5)(A).

144. By injecting code into third-party websites rendered within Facebook's in-app browser, Defendant intentionally accessed Plaintiffs' and Class Members' Apple Devices without authorization, and as a result of that conduct, caused or recklessly caused damage or loss to those protected computers, in violation of 18 U.S.C. §§ 1030(a)(5)(B) and (a)(5)(C).

145. Defendant's injection of code into third-party websites rendered within Facebook's in-app browser was a single act by which Defendant intentionally accessed Plaintiffs' and Class Members' protected computers without authorization and exceeding authorization. As a direct and proximate result of Defendant's CFAA violations, Defendant caused damages and loss to Plaintiffs and Class Members during a one-year period that exceed $5,000 in value.

146. Defendant's injection of code into third-party websites rendered within Facebook's in-app browser caused damage and loss to Plaintiffs and Class Members, including by decreasing the value of their private and personally identifiable information and communications, and by impeding their ability to control the dissemination and use of such information and communications, which they reasonably

believed would be protected from tracking and disclosure by result of the privacy controls they implemented on their devices.

147. Defendant's conduct also represents "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the sensitive, confidential information, including protected health information, that Meta collects and disseminates to its advertising partners and/or other third parties without adequate legal privacy protections.

148. Accordingly, Plaintiffs and Class Members may "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief" and hereby seek recovery of economic damages and all other relief provided for under 18 U.S.C. § 1030(g).

THIRD CLAIM FOR RELIEF

VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 630 *et seq.* ("CIPA")
(On Behalf of the Class or, Alternatively, the California Subclass)

149. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class or, alternatively, the California Subclass.

150. The California Invasion of Privacy Act , codified at Cal. Penal Code §§ 630-638, contains the following statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Penal Code § 630.

151. California Penal Code § 631(a) accordingly provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or

> permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

152. At all relevant times, Meta's business practices described herein allowed it to access, intercept, learn the contents of and collect Plaintiffs' and Class Members' personally identifiable information and other data, including information concerning their interactions with third-party websites, even when Plaintiffs' and Class Members' devices were set to block such actions.

153. Plaintiffs and Class Members, during one or more of their relevant interactions on the internet during the Class Period, communicated with one or more third-party websites owned by entities based in California, and whose servers were located in California, and also communicated with Meta's servers located in California. Communications from the California web-based entities to Plaintiffs and Class Members, and from Plaintiffs and Class Members to the California web-based entities, were sent to California and illegally intercepted by Meta.

154. Plaintiffs and Class Members did not consent to any of Meta's actions in intercepting, reading, and learning the contents of their communications with such California-based entities. Meta read and learned the contents of Plaintiffs' and Class Members' communications in transit and without authorization. Meta failed to disclose that it was intercepting, tracking and learning the contents of such private conversations and activities when it directed users, without their knowledge or consent, to external third-party websites from within the Facebook app.

155. Meta's conduct was intentional in that it purposefully diverted users to its in-app browser and installed code which allows it to monitor and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta. Meta directly participated in the interception, reading, and/or learning of the contents of the communications between Plaintiffs and Class Members and California-based web entities.

156. The information Meta intercepted while Plaintiffs and Class Members used the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords, birthdates, and payment card information), and how much time a user spent on which websites.

157. Meta intentionally intercepted Plaintiffs' and Class Members' information in transit. Meta intercepted Plaintiffs' and Class Members' website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute electronic communications and were contemporaneously copied by Meta in real time.

158. Plaintiffs and Class Members have experienced damage and loss by reason of these violations, including but not limited to, violation of their right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

159. As a result of the above violations and pursuant to CIPA section 637.2, Meta is liable to Plaintiffs and Class Members for the greater of treble actual damages related to their loss of privacy in an amount to be determined at trial, or statutory damages in the amount of $5,000 per violation. Section 637.2 provides "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

160. Plaintiffs further request, as provided under CIPA, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

FOURTH CLAIM FOR RELIEF

VIOLATION OF THE UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL")
(On Behalf of the Class or, Alternatively, the California Subclass)

161. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class or, alternatively, the California Subclass.

162. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

163. Meta is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

164. The acts and omissions complained of herein were conceived of and directed from, and emanated from, California.

165. By engaging in the acts and practices described herein, Meta has committed one or more acts of unfair, unlawful, or fraudulent competition violative of the UCL, and as a result, Plaintiffs and Class Members have suffered injury in fact and lost money and/or property through the insertion of JavaScript on their devices, as described herein, and the invasion and lost value of their personally identifiable information and other data.

Unlawful

166. Meta's conduct violates, among other enactments, the Wiretap Act, the Computer Fraud and Abuse Act, California's Invasion of Privacy Act, and Article I, Section I of the California Constitution. Consequently, Meta's conduct violates the unlawful prong of the UCL.

Unfair

167. Meta's conduct is substantially unfair, predatory and contrary to California's and the nation's legislatively declared public policy in favor of protecting the privacy and security of personal confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard."); California Bill Analysis, A.B. 375 Assem. (June 27, 2017) (noting that "[t]he unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.").

168. Meta acted in an unethical, unscrupulous, outrageous, oppressive, and substantially injurious manner. Meta engaged in unfair business practices and acts in at least the following respects:

(a) Without Plaintiffs' and Class Members' knowledge or consent, Meta injected code into every web URL opened through its in-app browser, which was capable of and engaged in overriding security and privacy settings previously set by Plaintiffs and Class Members; and

(b) Meta actively intercepted, viewed, and collected Plaintiffs' and Class Members' personally identifiable information to use it for advertising and other purposes for Meta's financial

benefit. The information and data Meta intercepted includes highly sensitive and valuable personal information, including but not limited to personally identifiable information, confidential medical facts, and other privileged communications and private details.

169. Plaintiffs interacted with various third-party websites reasonably believing that their browsing activities—and any facts and information communicated to third-party websites—were secure and confidential (i.e., solely between themselves and the third-party website).

170. There is no justification for Meta's conduct other than to increase, beyond what it would have otherwise realized, its profit from fees from third parties and the value of its information assets by acquisition of Plaintiffs' and Class Members' personal information. Meta's conduct lacks justification in that Meta has benefited from such conduct and practices while Plaintiffs and Class Members were misled as to the nature and integrity of Meta's services and were materially disadvantaged in regard to their interests in the privacy and confidentiality of their personal information.

Fraudulent

171. Meta's acts and practices were fraudulent in violation of the UCL because they were likely to, and did, in fact, mislead the members of the public to whom they were directed. Meta actively concealed its tracking practice at issue and had exclusive knowledge of it, creating a duty to disclose.

172. Meta failed to disclose this tracking practice. Its disclosure would have been a material and important factor in Plaintiffs' and Class Members' actions related to visiting third-party websites through Facebook's in-app browser or another browser.

173. Meta's secret, undisclosed, and deceptive tracking practice caused Plaintiffs and Class Members to surrender more in their transaction with Meta than they otherwise would have. Had Plaintiffs and Class Members known that Meta could and would use its in-app browser in the manner described, directly counter to their stated preference known to Meta, they would have avoided navigating to third-party websites from within Facebook, and instead would have copied and pasted links into their standard browser to avoid being tracked, thereby avoiding this injury.

174. Meta's conduct was unethical, deceptive and unscrupulous in part because it acted against the express, known wish of Plaintiffs and Class Members not to be tracked without communicating to them the material fact that Meta would, in fact, track their private browsing activities and

communications. Further, Meta's deceptive conduct narrowly benefitted its own business interests at the expense of Plaintiffs' and Class Members' fundamental privacy rights and interests protected by California's Constitution and common law.

175. Plaintiffs' and Class Members' loss of their personal information constitutes an economic injury. Plaintiffs and Class Members have a property right in their personal information, which has value to themselves as well as Meta, and lost money or property as a result of Defendant's violations of the UCL. Plaintiffs and Class Members have suffered harm in the form of lost property value, specifically the diminution of the value of their private and personally identifiable data and content, of which they lost control against their wishes. Meta's actions also caused damage to and loss of Plaintiffs' and Class Members' property right to control the dissemination and use of their personal information and communications.

176. Plaintiffs and Class Members accordingly seek appropriate relief, including (1) restitution under the UCL; and (2) such orders or judgments as may be necessary to enjoin Meta from continuing its unfair, unlawful, and fraudulent practices. There is no adequate remedy at law that would provide redress to Plaintiffs and Class Members or ensure that Meta, a serial privacy offender, will not continue engaging in the same practices. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law, including under California Code of Civil Procedure section 1021.5.

FIFTH CLAIM FOR RELIEF

VIOLATION OF THE FLORIDA SECURITY OF COMMUNICATIONS ACT
Fla. Stat. Ann. § 934.01 *et seq.* ("FSCA")
(On Behalf of the Florida Subclass)

177. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

178. Plaintiffs Lisa Bush and David Alzate bring this count individually and on behalf of the Florida Subclass.

179. The Florida Security of Communications Act is codified at Florida Statutes Annotated §§ 934.01–934.50. Florida Statutes Annotated § 934.03(1)(a) punishes, in pertinent part, any person who "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication."

180. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiffs Lisa Bush's and David Alzate's and Florida Subclass Members' electronic communications with third-party websites.

181. Without Plaintiffs Lisa Bush's and David Alzate's, Florida Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiffs Lisa Bush's and David Alzate's and Florida Subclass Members' electronic communications when they navigated to third-party websites within Facebook's in-app browser.

182. Meta contemporaneously intercepted the contents of Plaintiffs Lisa Bush's and David Alzate's and Florida Subclass Members' electronic communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

183. Meta intentionally used an electronic, mechanical, or other device—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiffs Lisa Bush's and David Alzate's and Florida Subclass Members' electronic communications, in violation of the FSCA.

184. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members were unaware that Facebook was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites.

185. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

186. The information Meta intercepted while Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

187. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

188. Meta intentionally intercepted Plaintiffs Lisa Bush's and David Alzate's and Florida Subclass Members' information in transit. Meta intercepted their website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute electronic communications and were contemporaneously copied by Meta in real time.

189. Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

190. As a result of the above violations and pursuant to Florida Statutes Annotated § 934.10, Meta is liable to the Plaintiffs Lisa Bush and David Alzate and Florida Subclass Members for the greater of their actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000.

191. Plaintiffs Lisa Bush and David Alzate further request, as provided under Florida Statutes Annotated § 934.10, reasonable attorneys' fees and costs of suit, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

SIXTH CLAIM FOR RELIEF

VIOLATION OF THE ILLINOIS EAVESDROPPING ACT
720 ILCS 5/14-1 *et seq.*
(On Behalf of the Illinois Subclass)

192. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

193. Plaintiffs Mark Letoski and Louis Green bring this count individually and on behalf of the Illinois Subclass.

194. A person violates the Illinois Eavesdropping Act where he or she "knowingly and intentionally . . . [i]ntercepts, records, or transcribes, in a surreptitious manner, any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication . . . ." 720 ILCS 5/14-2(a).

195. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept, record, or transcribe the contents of Plaintiffs Mark Letoski's and Louis Green's and Illinois Subclass Members' private electronic communications with third-party websites.

196. Without Plaintiffs Mark Letoski's, Louis Green's and Illinois Subclass Members', or third-party websites' knowledge or consent, Meta intercepted, recorded, or transcribed the contents of Plaintiffs Mark Letoski's and Louis Green's and Illinois Subclass Members' electronic communications when they navigated to third-party websites within Facebook's in-app browser.

197. Meta contemporaneously intercepted the contents of Plaintiffs Mark Letoski's and Louis Green's and Illinois Subclass Members' electronic communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

198. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

199. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members were unaware that Facebook was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites.

200. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

201. The information Meta intercepted while Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation,

every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

202. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

203. Meta intentionally intercepted Plaintiffs Mark Letoski's and Louis Green's and Illinois Subclass Members' information in transit. Meta intercepted their website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute electronic communications and were contemporaneously copied by Meta in real time.

204. Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

205. As a result of the above violations and pursuant to 720 ILCS 5/14-6, Meta is liable to the Plaintiffs Mark Letoski and Louis Green and Illinois Subclass Members for actual damages. Plaintiffs Mark Letoski and Louis Green further request, as provided under 720 ILCS 5/14-6 injunctive and declaratory relief and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

SEVENTH CLAIM FOR RELIEF

VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT
18 Pa. Stat. and Cons. Stat. Ann. § 5701 *et seq.* ("WESCA")
(On Behalf of the Pennsylvania Subclass)

206. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

207. Plaintiffs Chanel Robinson and Kevin bring this count individually and on behalf of the Pennsylvania Subclass.

208. The Pennsylvania Wiretapping and Electronic Surveillance Control Act makes it unlawful to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept any wire, electronic or oral communication." 18 Pa. Stat. and Cons. Stat. Ann. § 5703(1).

209. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiffs Chanel Robinson's and Kevin Zenstein's and Pennsylvania Subclass Members' electronic communications with third-party websites.

210. Without Plaintiffs Chanel Robinson's and Kevin Zenstein's, Pennsylvania Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiffs Chanel Robinson's and Kevin Zenstein's and Pennsylvania Subclass Members' electronic communications when they navigated to third-party websites within Facebook's in-app browser.

211. Meta contemporaneously intercepted the contents of Plaintiffs Chanel Robinson's and Kevin Zenstein's and Pennsylvania Subclass Members' electronic communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

212. Meta intentionally used an electronic, mechanical, or other device—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiffs Chanel Robinson's and Kevin Zenstein's and Pennsylvania Subclass Members' electronic communications, in violation of the WESCA.

213. Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members were unaware that Facebook was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites.

214. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

215. The information Meta intercepted while Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members were using Facebook's in-app browser includes personally

identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which website.

216. Meta intentionally intercepted Plaintiffs Chanel Robinson's and Kevin Zenstein's and Pennsylvania Subclass Members' information in transit. Meta intercepted their website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute electronic communications and were contemporaneously copied by Meta in real time.

217. Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

218. As a result of the above violations and pursuant to 18 Pennsylvania Statutes and Consolidated Statutes Annotated § 5725(a), Meta is liable to Plaintiffs Chanel Robinson and Kevin Zenstein and Pennsylvania Subclass Members for the greater of their actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000. Plaintiffs Chanel Robinson and Kevin Zenstein further request, as provided under 18 Pennsylvania Statutes and Consolidated Statutes Annotated § 5725(a), reasonable attorneys' fees and costs of suit and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

EIGHTH CLAIM FOR RELIEF

VIOLATION OF WASHINGTON'S PRIVACY ACT
Wash. Rev. Code Ann. § 9.73.030
(On Behalf of the Washington Subclass)

219. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

220. Plaintiffs Mary Thew and Lisa Evans bring this count individually and on behalf of the Washington Subclass.

221. Washington Revised Code Annotated § 9.73.030(1) provides, in pertinent part:

> [I]t shall be unlawful for any individual, partnership, corporation, [or] association . . . to intercept, or record any: (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.

222. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept or record the contents of Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' private communications with third-party websites.

223. Without Plaintiffs Mary Thew's and Lisa Evans's, Washington Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' private communications when they navigated to third-party websites within Facebook's in-app browser.

224. Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' private communications were transmitted to third-party websites via a device.

225. Meta contemporaneously intercepted the contents of Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' private communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

226. Meta intentionally used a device—the JavaScript code it injected into third-party websites—designed as a means of intercepting and acquiring the contents of Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' private communications, in violation of Washington Revised Code Annotated § 9.73.030(1).

227. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members were unaware that Facebook was intercepting its users' private communications and tracking their communications and interactions with third-party websites.

228. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

229. The information Meta intercepted while Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

230. Meta intentionally intercepted Plaintiffs Mary Thew's and Lisa Evans's and Washington Subclass Members' information in transit. Meta intercepted their website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other private communication. These communications constitute private communications and were contemporaneously copied by Meta in real time.

231. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

232. Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

233. As a result of the above violations and pursuant to Washington Revised Code Annotated § 9.73.060, Meta is liable to the Plaintiffs Mary Thew and Lisa Evans and Washington Subclass Members for actual damages, liquidated damages computed at the rate of $100 a day for each violation. Plaintiffs Mary Thew and Lisa Evans further request, as provided under Washington Revised Code Annotated § 9.73.060, reasonable attorneys' fees and costs of suit.

NINTH CLAIM FOR RELIEF

VIOLATION OF THE MISSOURI WIRETAP ACT
Mo. Stat. § 542.400 *et seq*.
(On Behalf of the Missouri Subclass)

234. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

235. Plaintiff Raven Johnson brings this count individually and on behalf of the Missouri Subclass.

236. The Missouri Wiretap Act is codified at Missouri Annotated Statutes §§ 542.400–542.424. Missouri Annotated Statutes § 542.402 punishes, in pertinent part, any person who "[k]nowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire communication."

237. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 542.400(9).

238. Defendant, as a corporation, is a "person" under the Missouri Act.

239. "Intercept" is defined as the "acquisition of the contents of any wire communication through the use of any electronic or mechanical device." *Id.* § 542.400(6).

240. "Contents" is defined as either "any information concerning the identity of the parties, the substance, purport, or meaning of that communication." *Id.* § 542.400(3).

241. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications." *Id.* § 542.400(12).

242. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiff Raven Johnson's and Missouri Subclass Members' wire communications with third-party websites.

243. Without Plaintiff Raven Johnson's, Missouri Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiff Raven Johnson's and Missouri Subclass Members' wire communications when they navigated to third-party websites within Facebook's in-app browser.

244. Meta contemporaneously intercepted the contents of Plaintiff Raven Johnson's and Missouri Subclass Members' wire communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

245. Meta intentionally used an electronic or mechanical device—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff Raven Johnson's and Missouri Subclass Members' wire communications, in violation of the Missouri Wiretap Act.

246. Plaintiff Raven Johnson and Missouri Subclass Members were unaware that Facebook was intercepting its users' wire communications and tracking their communications and interactions with third-party websites.

247. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

248. The information Meta intercepted while Plaintiff Raven Johnson and Missouri Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

249. Plaintiff Raven Johnson and Missouri Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

250. Meta intentionally intercepted Plaintiff Raven Johnson's and Missouri Subclass Members' information in transit. Meta intercepted their website communications whenever they used

Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute wire communications and were contemporaneously copied by Meta in real time.

251. Plaintiff Raven Johnson and Missouri Subclass Members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

252. As a result of the above violations and pursuant to Missouri Annotated Statutes § 542.418, Meta is liable to the Plaintiff Raven Johnson and Missouri Subclass Members for the greater of their actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $10,000.

253. Plaintiff Raven Johnson further requests, as provided under Missouri Annotated Statutes § 542.418, reasonable attorneys' fees and costs of suit, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

TENTH CLAIM FOR RELIEF

VIOLATION OF THE MASSACHUSETTS WIRETAP STATUTE
Mass. Gen. Laws Ann. 272 § 99
(On Behalf of the Massachusetts Subclass)

254. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

255. Plaintiff Ed Rennie brings this count individually and on behalf of the Massachusetts Subclass.

256. Massachusetts bars the surreptitious interception and recording of private communications. Mass Gen. Laws Ann. 272 § 99.

257. It is a violation of Massachusetts law for any person to willfully commit an interception, attempt to commit an interception, or procure any other person to commit an interception or attempt to commit an interception of any wire communication. *Id.* § 99(C)(1).

/ / /

/ / /

258. Further, it is a violation for any person to willfully use, or attempt to use, "the contents of any wire . . . communication, knowing that the information was obtained through interception." *Id.* § 99(C)(3)(b).

259. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 99(B)(13).

260. Defendant, as a corporation, is a "person" under Massachusetts law.

261. "Interception" is defined as "to secretly record . . . the contents of any wire . . . communications through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." *Id.* § 99(B)(4).

262. "Wire communication" is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." *Id.* § 99(B)(1).

263. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport, or meaning of that communication." *Id.* § 99(B)(5).

264. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiff Ed Rennie's and Massachusetts Subclass Members' wire communications with third-party websites.

265. Without Plaintiff Ed Rennie's, Massachusetts Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiff Ed Rennie's and Massachusetts Subclass Members' wire communications when they navigated to third-party websites within Facebook's in-app browser.

266. Meta contemporaneously intercepted the contents of Plaintiff Ed Rennie's and Massachusetts Subclass Members' wire communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

267. Meta intentionally used an electronic or mechanical device—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff Ed Rennie's and Massachusetts Subclass Members' wire communications, in violation of Massachusetts law.

268. Plaintiff Ed Rennie and Massachusetts Subclass Members were unaware that Facebook was intercepting its users' wire communications and tracking their communications and interactions with third-party websites.

269. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

270. The information Meta intercepted while Plaintiff Ed Rennie and Massachusetts Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

271. Plaintiff Ed Rennie and Massachusetts Subclass Members intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

272. Meta intentionally intercepted Plaintiff Ed Rennie's and Massachusetts Subclass Members' information in transit. Meta intercepted Plaintiff Ed Rennie's and Massachusetts Subclass Members' website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute wire communications and were contemporaneously copied by Meta in real time.

273. Plaintiff Ed Rennie and Massachusetts Subclass Members have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

274. As a result of the above violations and pursuant to Massachusetts General Laws Annotated Chapter 272, § 99(Q), Meta is liable to the Plaintiff Ed Rennie and Massachusetts Subclass Members for the greater of their actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000.

275. Plaintiff Ed Rennie further requests, as provided under Massachusetts General Laws Annotated Chapter 272, § 99(Q), reasonable attorneys' fees and costs of suit, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

ELEVENTH CLAIM FOR RELIEF

VIOLATION OF THE MARYLAND WIRETAP ACT
Md. Cts. & Jud. Pro. § 10-401 *et seq.*
(On Behalf of the Maryland Subclass)

276. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

277. Plaintiff Teia Pittman brings this count individually and on behalf of the Maryland Subclass.

278. The Maryland Wiretap Act bars the surreptitious interception and recording of private communications. Md. Cts. & Jud. Pro. § 10-402.

279. It is a violation of the Maryland Wiretap Act for any person to "[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* § 10-402(a)(1).

280. Further, it is a violation for any person to willfully use, or endeavor to use, "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication." *Id.* § 10-402(a)(3).

281. "Person" includes "any individual, partnership, association, joint stock company, trust, or corporation." *Id.* § 10-401(14).

282. Defendant, as a corporation, is a "person" under the Maryland Wiretap Act.

283. "Intercept" is defined as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 10- 401(10).

284. "Contents" is defined as either "any information concerning the identity of the parties to such communication," or any information concerning the "existence, contents, substance, purport, or meaning of that communication." *Id.* § 10-401(4).

285. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system." *Id.* § 10-401(5)(i).

286. At all relevant times, Meta's business practice of injecting its unique JavaScript code into third-party websites allowed it to intercept the contents of Plaintiff Teia Pittman's and Maryland Subclass Members' electronic communications with third-party websites.

287. Without Plaintiff Teia Pittman's, Maryland Subclass Members', or third-party websites' knowledge or consent, Meta intercepted the contents of Plaintiff Teia Pittman's and Maryland Subclass Members' electronic communications when they navigated to third-party websites within Facebook's in-app browser.

288. Meta contemporaneously intercepted the contents of Plaintiff Teia Pittman's and Maryland Subclass Members' electronic communications while they were in transit and without authorization. Meta failed to disclose that it was intercepting and tracking the contents of such private conversations and activities when users visit external third-party websites from within the Facebook app.

289. Meta intentionally used an electronic or mechanical device—the JavaScript code it injected into third-party websites—as a means of intercepting and acquiring the contents of Plaintiff Teia Pittman's and Maryland Subclass Members' electronic communications, in violation of the Maryland Wiretap Act.

290. Plaintiff Teia Pittman and Maryland Subclass Members were unaware that Facebook was intercepting its users' electronic communications and tracking their communications and interactions with third-party websites.

291. Meta's conduct was intentional in that it purposefully installed code which allows it to intercept and learn the content of its users' communications and other browsing activities that would otherwise be unavailable to Meta.

292. The information Meta intercepted while Plaintiff Teia Pittman and Maryland Subclass Members were using the Facebook in-app browser includes personally identifiable information and other highly specific information and communications, including, without limitation, every button, keystroke and link a user taps, whether the user has taken any screenshots, text entries (including passwords and credit card information), and how much time a user spent on which websites.

293. Plaintiff Teia Pittman and Maryland Subclass Member intended and believed that the information they provided to third-party websites while using Facebook's in-app browser would remain private and would not be transmitted to Meta.

294. Meta intentionally intercepted Plaintiff Teia Pittman's and Maryland Subclass Members' information in transit. Meta intercepted their website communications whenever they used Facebook's in-app browser to communicate with third-party websites using the JavaScript code inserted by Meta, including every mouse movement, click, keystroke (e.g., text being entered into an information field or text box), URL visited, and other electronic communication. These website communications constitute electronic communications and were contemporaneously copied by Meta in real time.

295. Plaintiff Teia Pittman and Maryland Subclass Member have experienced damage and loss by reason of these violations, including but not limited to, violation of the right to privacy. Unless restrained and enjoined, Meta will continue to commit such acts.

296. As a result of the above violations and pursuant to Maryland Code Annotated, Courts & Judicial Proceedings § 10-410, Meta is liable to Plaintiff Teia Pittman and Maryland Subclass Members for the greater of their actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation, or $1,000.

297. Plaintiff Teia Pittman further requests, as provided under Maryland Code Annotated, Courts & Judicial Proceedings § 10-410, reasonable attorneys' fees and costs of suit, and punitive damages in an amount to be determined by a jury sufficient to prevent or deter the same or similar conduct by Meta.

/ / /

/ / /

TWELFTH CLAIM FOR RELIEF

INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of the Class or, Alternatively, Each State Subclass)

298. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class or, alternatively, each state subclass.

299. Plaintiffs and Class Members had a reasonable expectation of privacy when communicating with third-party websites, and, as a result of Meta's actions, they have suffered harm and injury, including from the invasion of their privacy rights.

300. By intercepting Plaintiffs' and Class Members' wire and electronic communications on the internet, Meta intentionally intruded upon their solitude or seclusion.

301. Meta's intentional intrusion on Plaintiffs' and Class Members' solitude or seclusion is highly offensive to a reasonable person, especially considering the extremely personal, sensitive, and confidential information and data that Meta monitored, intercepted, transmitted and recorded in spite of Plaintiffs' and Class Members' known, expressed preference not to have this information tracked.

302. Meta's conduct infringed Plaintiffs' and Class Members' privacy interests in, among other things, (1) preventing the dissemination and/or misuse of their sensitive, confidential personally identifiable information; (2) maintaining control over the type of information that Meta tracks and/or records; and (3) making personal decisions and/or conducting personal activities without observation, intrusion, or interference, including being able visit and interact with various internet sites without that information being intercepted by Meta without Plaintiffs' and Class Members' knowledge or consent.

303. Plaintiffs and Class Members have been damaged as a direct and proximate result of Meta's invasion of their privacy rights and are entitled to just compensation, including monetary damages, in an amount to be determined at trial.

THIRTEENTH CLAIM FOR RELIEF

INVASION OF PRIVACY (PUBLICATION OF PRIVATE FACTS)
(On Behalf of the Class or, Alternatively, Each State Subclass)

304. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class or, alternatively, each state subclass.

305. Plaintiffs' and Class Members' personal information, including their Internet communications and sensitive data, are private facts that Meta acquired without the knowledge or consent of Plaintiffs and Class Members.

306. Meta gave publicity to Plaintiffs' and Class Members' private facts and the content of their Internet communications by sharing and selling them to its advertising partners. Many of those companies have business models predicated on building massive databases of individual consumer profiles from which to sell, broker or display targeted advertising.

307. Plaintiffs and Class Members had no knowledge that Meta was collecting, selling, and publishing to such third parties their private browsing activities and overriding their privacy settings because they had opted out of such tracking and did not otherwise consent to being tracked on third-party websites.

308. Meta's surreptitious tracking and commoditization of Plaintiffs' and Class Members' personal information would be highly offensive to a reasonable person, particularly because Plaintiffs chose to opt out of tracking to prevent Meta or its advertising partners from viewing, acquiring, and using their personal information.

309. In disseminating Plaintiffs' and Class Members' personal information without their consent in the manner described above, Meta acted with oppression, fraud, or malice.

310. Plaintiffs and Class Members have been damaged by the publication of their private information and are entitled to just compensation in the form of actual damages, general damages, unjust enrichment, nominal damages, and punitive damages.

FOURTEENTH CLAIM FOR RELIEF

UNJUST ENRICHMENT
(On Behalf of the Class or, Alternatively, Each State Subclass)

311. Plaintiffs incorporate the above allegations by reference as if fully set forth herein and bring this count individually and on behalf of the Class or, alternatively, each state Subclass under universal principles in equity.

312. Plaintiffs lack an adequate remedy at law.

313. Plaintiffs and Class Members conferred benefits on Meta by using Facebook and by consequence of Meta's receipt of their personal and confidential information, including through the tracking practices challenged in this case.

314. As set forth herein, Meta secretly intercepts, monitors, and records Facebook users' online activity and communications with external third-party websites by injecting code into those sites. When users click on a link within the Facebook app, Meta automatically directs them to the in-app browser that it is monitoring, rather than to their default browser, without telling the users this is happening or they are being tracked, even where users expressly indicated they do not consent to being tracked and their other relevant settings would block such tracking. Meta engages in such conduct to reap profits from exploiting its users' confidential personal information, despite all Plaintiffs and Class Members declining to consent to having their information so exploited.

315. Meta acquired the personal information of Plaintiffs and Class Members by deceit and in direct contravention of their expressed wishes to opt out of Meta tracking.

316. Equity and good conscience militate against permitting Meta to retain the profits and benefits from its wrongful conduct, which should be restored to Plaintiffs and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class and Subclasses defined herein, respectfully request that this Court:

A. Certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoint Plaintiffs and their attorneys to represent the Class;

B. Award compensatory damages, including statutory damages where available, and/or restitution to Plaintiffs and Class Members against Meta in an amount to be proven at trial, in addition to interest thereon;

C. Award punitive damages in an amount sufficient to prevent or deter the same or similar conduct by Meta;

D. Permanently restrain Meta, and its officers, agents, servants, employees and attorneys, from injecting JavaScript into third-party websites in a manner that allows Meta to intercept

users' private communications and track users' internet activity on third-party websites in a manner that is inconsistent with their privacy settings or preferences;

E. Award Plaintiffs and Class Members their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

F. Grant such other and further relief as the Court deems appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury for all claims so triable.

Dated: February 6, 2023

Respectfully submitted,

By: /s/ *Adam E. Polk*

Adam E. Polk (SBN 273000)
Simon S. Grille (SBN 294914)
Kimberly Macey (SBN 342019)
Reid Gaa (SBN 330141)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com
rgaa@girardsharp.com

Gary M. Klinger (*pro hac vice* forthcoming)
Nick Suciu (*pro hac vice* forthcoming)
Alexandra M. Honeycutt (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com
nsuciu@milberg.com
ahoneycutt@milberg.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
jnelson@milberg.com